JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: **10145360**
(43)Date of publication of application: **29.05.1998**

(51)Int.Cl.

H04L 12/22
H04L 12/28
H04L 12/24
H04L 12/26

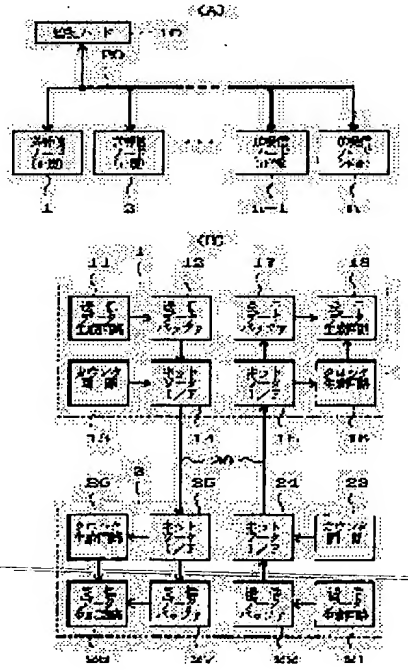
(21)Application number: **08307320**
(22)Date of filing: **01.11.1996**

(71)Applicant: **YAMAHA CORP**
(72)Inventor: **FUJIMORI JUNICHI**

(54) PREVENTION SYSTEM OF WRONG COPY, MONITORING NODE AND TRANSMITTING AND RECEIVING NODE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the transfer of data to a wrong equipment, without changing the data themselves via the encryption processing, etc.
SOLUTION: Each of normal nodes 1 to 1−n has a normal data input/output operation mode, in which the input/output of data is carried out with no application of the data processing, such as the encryption processing, and a protection data input/output operation mode where a wrong node (n) protects the fetching of data. The latter operation mode includes two modes, i.e., a mode where the data which has undergone the encipherment processing are inputted and outputted via a network 20, and the other mode where no input/output of data are carried out via a network 20. Thus, a communication network is constructed by connecting plural normal nodes, so that the input/output of data are freely carried out among the normal nodes. When the connection of a wrong node is detected, a monitoring node 10 gives a command to a group of normal nodes to perform the input/output of data in a protection data input/output operation mode.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

MENU SEARCH INDEX DETAIL

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－145360

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ 12/22		Ｈ０４Ｌ 11/26		
12/28		11/00	３１０Ｄ	
12/24		11/08		
12/26				

審査請求　未請求　請求項の数17　ＦＤ　（全 14 頁）

(21)出願番号　特願平8－307320

(22)出願日　平成８年(1996)11月１日

(71)出願人　000004075
ヤマハ株式会社
静岡県浜松市中沢町10番１号

(72)発明者　藤森　潤一
静岡県浜松市中沢町10番１号　ヤマハ株式会社内

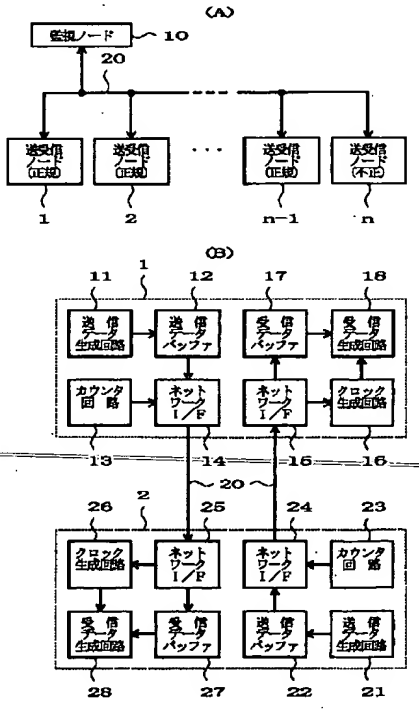
(74)代理人　弁理士　飯塚　義仁

(54)【発明の名称】　不正コピー防止システム、監視ノード及び送受信ノード

(57)【要約】　（修正有）

【課題】　データ自体を暗号化処理などで変更しなくても、不正な機器とのデータの送受を防ぐ。

【解決手段】　正規ノード１～ｎ－１は、暗号化処理などのデータ処理を施すことなくデータを入出力する通常のデータ入出力動作モードと、不正ノードｎがデータの取込みを防ぐプロテクトデータ入出力動作モードとを具える。プロテクトデータ入出力動作モードには暗号化処理されたデータをネットワーク２０上に入出力するものと、ネットワーク経由でデータの入出力動作を行わないものとがある。このような正規ノードの複数を接続し、それぞれの正規ノード間でデータの入出力動作を自由に行えるように通信ネットワークを構成する。監視ノード１０は、不正ノードが接続されたことを検出した場合、正規ノード群に対してプロテクトデータ入出力動作モードでデータの入出力動作を行うように指令を出す。



【特許請求の範囲】

【請求項１】　暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むことができないようにするプロテクトデータ入出力動作モードとを具えた複数の正規ノード群と、

この複数の正規ノード群を接続し、それぞれの正規ノード間でデータの入出力動作を自由に行えるように構成された通信ネットワークと、

前記通信ネットワークに接続されており、前記通信ネットワークに不正ノードが新たに接続されたことを検出した場合に、前記複数の正規ノード群に対して前記プロテクトデータ入出力動作モードでデータの入出力動作を行うように指令を出す監視ノードとを具備することを特徴とする不正コピー防止システム。

【請求項２】　暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むことができないようにするプロテクトデータ入出力動作モードとを具えた複数の正規ノード群と、

この正規ノードとの間でデータのやりとりを行うことを許可されていない不正ノードと、

前記正規ノードと前記不正ノードがそれぞれ少なくとも１つずつ接続されて構成された通信ネットワークと、

前記通信ネットワークに後から接続され、前記不正ノードが接続されていることを検出した場合に、前記通信ネットワークに接続されている前記正規ノードに対して前記プロテクトデータ入出力動作モードでデータの入出力動作を行うように指令を出す監視ノードとを具備することを特徴とする不正コピー防止システム。

【請求項３】　前記監視ノードは、前記通信ネットワークに予め接続されており、前記通信ネットワーク上に前記正規ノード又は不正ノードが新たに接続された場合に前記通信ネットワークに不正ノードが接続されているかどうかの検出を行うことを特徴とする請求項２に記載の不正コピー防止システム。

【請求項４】　前記監視ノードは、前記通信ネットワークに予め接続されており、前記通信ネットワークに正規ノード又は不正ノードが新たに接続されたことを前記通信ネットワークに予め接続されている前記正規ノードからの確認信号に基づいて認識することを特徴とする請求項３に記載の不正コピー防止システム。

【請求項５】　前記監視ノードは、自分自身が前記通信ネットワークに後で接続された場合に前記通信ネットワークに不正ノードが接続されているかどうかの検出を行うことを特徴とする請求項２に記載の不正コピー防止システム。

【請求項６】　前記監視ノードは、機密化された暗号コードを前記通信ネットワーク上に出力することによって前記正規ノードから正規の機器である旨の返答を受け取り、その返答に応じて前記通信ネットワークに前記不正ノードが接続されているかどうかの検出を行うことを特徴とする請求項１、２、３、４又は５に記載の不正コピー防止システム。

【請求項７】　前記プロテクトデータ入出力動作モードとして、暗号化処理の施されたディジタルデータを通信ネットワーク上に入出力することによって不正ノードがディジタルデータを取り込むことができないようにすることを特徴とする請求項１又は２に記載の不正コピー防止システム。

【請求項８】　前記プロテクトデータ入出力動作モードは、通信ネットワーク経由でディジタルデータの入出力動作を行わないことによって不正ノードがディジタルデータを取り込むことができないようにすることを特徴とする請求項１又は２に記載の不正コピー防止システム。

【請求項９】　正規ノード及び不正ノードによって構成された通信ネットワーク上に機密化された暗号コードを出力することによって前記正規ノードから正規の機器である旨の返答を受け取り、その返答に応じて前記通信ネットワークに前記不正ノードが接続されていることを検出する不正ノード検出処理を行うことを特徴とする監視ノード。

【請求項１０】　前記通信ネットワークに正規ノード又は不正ノードが新たに接続されたことを検出して、前記不正ノード検出処理を行うことを特徴とする請求項９に記載の監視ノード。

【請求項１１】　前記通信ネットワークに正規ノード又は不正ノードが新たに接続されたことを前記通信ネットワークに予め接続されている前記正規ノードからの確認信号に応じて前記不正ノード検出処理を行うことを特徴とする請求項１０に記載の監視ノード。

【請求項１２】　少なくとも１つの正規ノードだけで構成された、又は正規ノードと不正ノードがそれぞれ少なくとも１つずつ接続されて構成された通信ネットワーク上に、正規ノード又は不正ノードが新たに接続された場合に、前記通信ネットワークに予め接続されている前記正規ノードから出力される確認信号に応じて前記通信ネットワークに前記不正ノードが接続されていることを検出する不正ノード検出処理を行うことを特徴とする監視ノード。

【請求項１３】　暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むことができないようにするプロテクトデータ入出力動作モードとを具え、正規ノード及び不正ノードによって構成された通信ネットワーク上に機密化された暗号コードを出力することによって前記正規ノードから正規の機器である旨の返答を受け取り、その返答

に応じて前記通信ネットワークに前記不正ノードが接続されていることを検出し、前記プロテクトデータ入出力動作モードでデータの入出力動作を行うように制御する送受信ノード。

【請求項１４】　請求項１３に記載の送受信ノードの複数を接続することによって構成された通信ネットワークからなる不正コピー防止システム。

【請求項１５】　暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むことができないようにするプロテクトデータ入出力動作モードとを具え、通信ネットワーク上に新たなノードが接続された場合に、その旨の確認信号を前記通信ネットワーク上に出力することを特徴とする送受信ノード。

【請求項１６】　前記プロテクトデータ入出力動作モードとして、暗号化処理の施されたディジタルデータを通信ネットワーク上に入出力することによって不正ノードがディジタルデータを取り込むことができないようにすることを特徴とする請求項１３又は１５に記載の送受信ノード。

【請求項１７】　前記プロテクトデータ入出力動作モードは、通信ネットワーク経由でディジタルデータの入出力動作を行わないことによって不正ノードがディジタルデータを取り込むことができないようにすることを特徴とする請求項１３又は１５に記載の送受信ノード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ディジタルオーディオデータなどの不正コピーを防止するコピー防止システムに関する。

【０００２】

【従来の技術】ディジタルデータの不正なコピーを防止する不正コピー防止システムとして、従来は送信機器側でディジタルデータ自体にスクランブルなどのデータ暗号化処理を施し、受信機器側でそのデータ暗号化処理を解読して元のディジタルデータを復号するスクランブル方式や、ディジタルデータのヘッダなどに予め付加されたＩＤ情報に基づいて、送信機器側又は受信機器側が通常のコピーなのか不正コピーなのかの判断を行い、その判断結果に基づいて送信又は受信を行わないように動作するＩＤ方式などが存在する。

【０００３】

【発明が解決しようとする課題】上述のスクランブル方式は、データ自体が暗号化処理によって変更されているので、送信機器側で暗号化処理を行わなければならないし、受信機器側でも受信又は再生時に解読処理を行わなければならない。すなわち、送信機器側及び受信機器側で暗号化に伴う過重の処理を行わなければならないという問題がある。一方、上述のＩＤ方式は、送信機器側又は受信機器側のいずれか一方にＩＤ情報自体を書き換えたりする不正な機器や、受信機器側にＩＤ情報を無視する不正な機器を用いた場合には、もはやＩＤ情報に基づいて不正なコピーを防止することはできないという問題を有する。この発明は上述の点に鑑みてなされたもので、データ自体を暗号化処理などで変更しなくても、不正な機器との間におけるデータのやりとりを行えないようにした不正コピー防止システムを提供するものである。また、この発明は、このような不正コピー防止システムを構成することのできる監視ノード及び送受信ノードを提供するものである。

【０００４】

【課題を解決するための手段】請求項１に記載の不正コピー防止システムは、暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むことができないようにするプロテクトデータ入出力動作モードとを具えた複数の正規ノード群と、この複数の正規ノード群を接続し、それぞれの正規ノード間でデータの入出力動作を自由に行えるように構成された通信ネットワークと、前記通信ネットワークに接続されており、前記通信ネットワークに不正ノードが新たに接続されたことを検出した場合に、前記複数の正規ノード群に対して前記プロテクトデータ入出力動作モードでデータの入出力動作を行うように指令を出す監視ノードとを具備するものである。正規ノードは、データ入出力モードとして、通常モードとプロテクトモードを有する。正規ノードだけで構成された通信ネットワーク上では、通常モードで自由にデータの入出力動作を行う。この通信ネットワーク上には監視ノードが接続されているので、不正ノードが接続されると、それを監視ノードが検出し、各正規ノード群にプロテクトモードでのデータ入出力動作を行うように指令を出すので、各正規ノードはプロテクトモードでデータ入出力動作を行うようになるので、不正ノードによるデータの不正コピーを有効に防止することが可能となる。

【０００５】請求項２に記載の不正コピー防止システムは、暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むことができないようにするプロテクトデータ入出力動作モードとを具えた正規ノードと、この正規ノードとの間ではデータのやりとりを行ってはいけない不正ノードと、前記正規ノードと前記不正ノードがそれぞれ少なくとも１つずつ接続されて構成された通信ネットワークと、前記通信ネットワークに後から接続され、前記不正ノードが接続されていることを検出した場合に、前記通信ネットワークに接続されている前記正規ノードに対して前記プロテクトデータ入出力動作モードでデータの入出力動作を行うように指令を出す監視ノードとを具備す

るものである。通信ネットワーク上には正規ノードと不正ノードとが少なくとも１つずつ接続されている。従って、本来このような通信ネットワーク上では通常データ入出力動作を行ってはいけないことになる。そこで、このようなネットワーク上に後から監視ノードを接続することによって、不正ノードを検出し、これ以降のデータ入出力動作モードでプロテクトモードにすることによって、不正ノードによる不正コピーを防止する。

【０００６】請求項３に記載の不正コピー防止システムは、請求項２に記載の不正コピー防止システムにおいて、前記監視ノードが、前記通信ネットワークに予め接続されており、前記通信ネットワーク上に前記正規ノード又は不正ノードが新たに接続された場合に前記通信ネットワークに不正ノードが接続されているかどうかの検出を行うようにしたものである。請求項４に記載の不正防止コピーシステムは、請求項３に記載の不正コピー防止システムにおいて、前記監視ノードが、前記通信ネットワークに予め接続されており、前記通信ネットワークに正規ノード又は不正ノードが新たに接続されたことを前記通信ネットワークに予め接続されている前記正規ノードからの確認信号に基づいて認識するようにしてものである。請求項５に記載の不正コピー防止システムは、請求項２に記載の不正コピー防止システムにおいて、前記監視ノードが、自分自身が前記通信ネットワークに後で接続された場合に前記通信ネットワークに不正ノードが接続されているかどうかの検出を行うようにしてものである。請求項３～５では、監視ノードがどのようなタイミングで通信ネットワーク上に接続されている不正ノードの存在を検出するのかを規定してものである。

【０００７】請求項６に記載の不正コピー防止システムは、請求項１、２、３、４又は５に記載の不正コピー防止システムにおいて、前記監視ノードが、機密化された暗号コードを前記通信ネットワーク上に出力することによって前記正規ノードから正規の機器である旨の返答を受け取り、その返答に応じて前記通信ネットワークに前記不正ノードが接続されているかどうかの検出を行うようにしてものである。監視ノードと正規ノードとの間の正規の機器であるかどうかの判定方法として、機密化された暗号コードを用いることによって、不正ノードにその内容を把握されないようにでき、不正コピーを有効に防止することができる。請求項７に記載の不正コピー防止システムは、請求項１又は２に記載のプロテクトデータ入出力動作モードとして、暗号化処理の施されたディジタルデータを通信ネットワーク上に入出力するものである。これによって、暗号化処理を行うことのできない不正ノードが通信ネットワークに接続された場合でも、そこを流れるディジタルデータが不正ノードに読み取られることはない。請求項８に記載の不正コピー防止システムは、請求項１又は２に記載のプロテクトデータ入出力動作モードとして、通信ネットワーク経由でディジタルデータの入出力動作を行わないものである。従って、正規ノード同士でディジタルデータのやりとりを行う場合には、両者間で専用回線を使って行えばよい。

【０００８】請求項９に係る監視ノードは、正規ノード及び不正ノードによって構成された通信ネットワーク上に機密化された暗号コードを出力することによって前記正規ノードから正規の機器である旨の返答を受け取り、その返答に応じて前記通信ネットワークに前記不正ノードが接続されていることを検出する不正ノード検出処理を行うものである。この監視ノードは、機密化された暗号コードを用いているので、不正ノードにその内容を把握されないように不正コピーを有効に防止することができる。また、機密化された暗号コードを不正ノードの接続された通信ネットワーク上に出力することによって、容易に不正ノードの存在を検出することができる。請求項１０に記載の監視ノードは、請求項９に記載の監視ノードにおいて、前記通信ネットワークに正規ノード又は不正ノードが新たに接続されたことを検出して、前記不正ノード検出処理を行うようにしたものである。これによって、監視ノードは、通信ネットワーク上に新たに正規ノード又は不正ノードのいずれか１つが接続された場合に不正ノード検出処理を行い、無駄に不正ノード検出処理動作を行わなくてもよい。請求項１１に記載の監視ノードは、請求項１０に記載の監視ノードにおいて、前記通信ネットワークに正規ノード又は不正ノードが新たに接続されたことを前記通信ネットワークに予め接続されている前記正規ノードからの確認信号に応じて前記不正ノード検出処理を行うようにしてものでなる。これによって、監視ノードが通信ネットワーク上を常に監視して、新たにノードが接続されたかどうかの新規ノード検出処理を行わなくてもよい。また、通信ネットワーク上に予め接続されている正規ノードにその新規ノード検出処理を分散させて行わせているので、監視ノードの処理負担を軽減することができる。請求項１２に記載の監視ノードは、少なくとも１つの正規ノードだけで構成された、又は正規ノードと不正ノードがそれぞれ少なくとも１つずつ接続されて構成された通信ネットワーク上に、正規ノード又は不正ノードが新たに接続された場合に、前記通信ネットワークに予め接続されている前記正規ノードから出力される確認信号に応じて前記通信ネットワークに前記不正ノードが接続されていることを検出する不正ノード検出処理を行うものである。監視ノードは、通信ネットワーク上に新たに正規ノード又は不正ノードのいずれか１つが新たに接続された場合に不正ノード検出処理を行い、無駄に不正ノード検出処理動作を行わなくてもよい。

【０００９】請求項１３に記載の送受信ノードは、暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むこと

ができないようにするプロテクトデータ入出力動作モードとを具え、正規ノード及び不正ノードによって構成された通信ネットワーク上に機密化された暗号コードを出力することによって前記正規ノードから正規の機器である旨の返答を受け取り、その返答に応じて前記通信ネットワークに前記不正ノードが接続されていることを検出し、前記プロテクトデータ入出力動作モードでデータの入出力動作を行うものである。この送受信ノードは、前述の監視ノードのように不正ノード検出処理動作を行うことができるものである。従って、特別な監視ノートを通信ネットワーク上に設けなくても不正ノードを検出でき、不正コピーを有効に防止することが可能となる。請求項１４に記載の不正コピー防止システムは、請求項１３に記載の送受信ノードの複数を接続することによって構成された通信ネットワークからなるものである。請求項１３に記載の送受信ノード自身が不正ノード検出処理動作を行うことができるので、これを用いて通信ネットワークを構成することによって容易に不正コピーを防止可能なシステムを構成することができる。請求項１５に記載の送受信ノードは、暗号化処理などのデータ処理を施すことなくそのままの形でディジタルデータを入出力する通常データ入出力動作モードと、不正ノードがディジタルデータを取り込むことができないようにするプロテクトデータ入出力動作モードとを具え、通信ネットワーク上に新たなノードが接続された場合に、その旨の確認信号を前記通信ネットワーク上に出力するものである。このような送受信ノードによって通信ネットワークを構成すると、監視ノードは通信ネットワーク上を常に監視して、新たにノードが接続されたかどうかの新規ノード検出処理を行わなくてもよく、監視ノードの処理負担を大幅に軽減することができる。請求項１６に記載の送受信ノードは、請求項１３又は１５に記載のプロテクトデータ入出力動作モードとして、暗号化処理の施されたディジタルデータを通信ネットワーク上に入出力するものである。これによって、暗号化処理を行うことのできない不正ノードが通信ネットワーク上に接続された場合でも、不正ノードは通信ネットワーク上を流れるディジタルデータを読み取ることはできない。請求項１７に記載の送受信ノードは、請求項１３又は１５に記載のプロテクトデータ入出力動作モードとして、通信ネットワーク経由でディジタルデータの入出力動作を行わないものである。従って、送受信ノードが正規ノード同士の場合には、両者間で専用回線を使ってディジタルデータのやりとりを行えばよい。

【００１０】

【発明の実施の形態】以下、添付図面を参照して、この発明の実施の形態を詳細に説明する。図１はこの発明に係る不正コピー防止システムの一実施の形態の全体構成を示す概略ブロック図である。図２はこの不正コピー防止システムによって伝送されるデータの構成例を示す図である。なお、本明細書中では、ＩＥＥＥ１３９４の通信方式に従ってデータ伝送が行われる場合を例に説明する。図１（Ａ）に示すように全部でｎ個の送受信ノード１～ｎと、１個の監視ノード１０が通信ネットワーク２０を介して接続されている。ここで、通信ネットワーク２０はバス形式のものでもよく、各送受信ノードが個別の通信回線を介して接続され、相互に通信ネットワーク２０を形成しているものであってもよい。以下では、説明の便宜上、図１（Ｂ）のように送受信ノード１と送受信側ノード２との間のデータ伝送について説明する。これ以外にも多数の送受信ノードが接続されているので、これらの間でも同様にしてデータ伝送が行われることはいうまでもない。この実施の形態では、送受信ノードｎ－１が図２のようなノーマルサイクルピリオド１２５μｓｅｃの同期信号（ｃｙｃｌｅ　ｓｙｎｃ）に対応したサイクルスタートパケット信号を順次出力している場合において、送受信ノード１が図２のようなデータ列を通信ネットワーク２０に送信し、そのデータ列９を送受信ノード２が受信して再現する場合について説明する。

【００１１】送受信ノード１において、送信データ生成回路１１は、図示していない内蔵の水晶発振器によって生成された所定周波数（例えば、周波数２４．５７６ＭＨｚ（周期約４０ｎｓｅｃ））のクロックに応じて動作し、所定のサンプリング周期Ｔの時系列的な配列を持つ複数のデータを順次生成し、出力するもので、例えば、ディジタルオーディオ信号の順次サンプルデータを出力する。例えば、送信データ生成回路１１は、ＤＡＴ（Ｄｉｇｉｔａｌ　Ａｕｄｉｏ　Ｔａｐｅ　ｒｅｃｏｄｅｒ）のようなオーディオ記録再生装置を含んでいてもよいし、あるいは楽音サンプルデータをリアルタイムで合成する楽音合成装置のようなものを含んでいてもよい。送信データ生成回路１１から出力されるデータのサンプリング周期Ｔは、そのデータソースに応じて、適宜可変されるようになっていてもよい。

【００１２】送信データ生成回路１１から出力されたデータは、その時系列順に送信データバッファ１２に一時的に記憶される。送信データバッファ１２は非同期で入出力動作するバッファレジスタである。カウンタ回路１３は、タイムスタンプデータすなわち時間データを作成するものであり、図示してない水晶発振器によって生成された所定周波数のクロックをカウントする３２ビット構成のランニングカウンタのようなものである。ネットワークインターフェイス１４は、所定の送信割り込み周期（前述の送受信ノードｎ－１の出力する同期信号（ｃｙｃｌｅ　ｓｙｎｃ））に同期して送信データバッファ１２に一時的に記憶してあるデータを基にして図２のような１アイソクロノスサイクル（ｉｓｏｃｈｒｏｎｏｕｓ　ｃｙｃｌｅ）に相当するデータ列９（以下「サイクルパケット列」とする）を構成し、それを通信ネットワーク２０に送信する。

【００１３】サイクルパケット列９は図２に示すように、サイクルスタートパケット９１と同期データパケット群９２と非同期データパケット群９３とから構成される。サイクルスタートパケット９１は、３２ビットで構成され、その上位２０ビットがそのサイクルパケット列９のサイクルタイミングを示すデータであり、下位１２ビットがそのサイクルパケット列９が通信ネットワーク２０上の同期信号（ｃｙｃｌｅ　ｓｙｎｃ）からどれだけの時間遅れで送信されたのかを示すサイクルスタートデータＸを示すデータである。同期データパケット群９２は擬似同期信号処理の対象となる複数Ｐ個のパケットデータで構成される。図では、一例としてチャンネルＪからチャンネルＮまでの５個の同期データパケットが示されている。この同期データパケットの数Ｐは任意に設定可能である。さらに、各同期データパケットは所定数Ｑ個のデータと、その中のいずれか１つ（この実施の形態では、最初のデータ）の時間位置を示すタイムスタンプデータとからなるグループを複数個有する。この実施の形態では、４個のデータと、１個のタイムスタンプで１つのグループが構成される。すなわち、図では、４個のデータＤ１～Ｄ４、Ｄ５～Ｄ８に対して１個のタイムスタンプデータＴ１、Ｔ２がそれぞれ設けられている。タイムスタンプデータＴ１は最初のデータＤ１の時間位置を、タイムスタンプデータＴ２はデータＤ５の時間位置をそれぞれ示す。従って、各同期データパケットは（Ｑ＋１）個のデータグループの整数倍で構成される。なお、ディジタルオーディオデータを通信する関係上、データがＱ個に満たなくても送信する場合があるがこれについては詳細説明を省略する。非同期データパケット群９３は非同期信号処理の対象となる複数Ｒ個のパケットデータで構成される。図では一例としてパケットＢ及びパケットＣの２個のパケットデータが示されている。なお、非同期データパケットは存在していなくてもよい。

【００１４】送受信ノード2において、ネットワークインターフェイス２４は通信ネットワーク２０を介して送信されてきたサイクルパケット列９を受信し、それを受信した順番で時系列的に受信データバッファ２７に一時的に記憶する。受信データバッファ２７は、非同期で入出力動作するバッファレジスタである。クロック生成回路２６は、受信したサイクルパケット列９のサイクルスタートパケットの中のサイクルスタートデータＸに基づいて、送受信ノード１の送信データ生成回路１１から供給されたデータと同じオリジナルのサンプリング周期Ｔを再現するものである。受信データ生成回路２８は、クロック生成回路２３から与えられる再現されたサンプリング周期Ｔに従い、受信データバッファ２８に一時的に記憶されているデータを順次読み出して再生する。読み出されたデータは適宜利用される。再生されたデータを如何なる形態で利用するかは、任意である。例えば、そのままＤ／Ａ変換してからスピーカ等から発音するようにしてもよいし、あるいは、エフェクト等の処理を施してからスピーカ等から発音する若しくは処理済みのデータを外部に送出するようにしてもよい。なお、送受信ノード１が受信側、送受信ノード２が送信側として動作する場合には、ネットワークインターフェイス２４、通信ネットワーク２０及びネットワークインターフェイス１５を介して同様の処理が行われる。

【００１５】次に、監視ノード１０の動作について図３のフローチャートを用いて説明する。この監視ノード１０は送受信ノード１～ｎ－１で構成された通信ネットワーク２０に予め接続されているものとする。監視ノード１０は、通信ネットワーク２０に送受信ノード（新規追加ノード）ｎが新たに接続されるまで、ステップ３１の処理を繰り返し実行する。ステップ３１で新規追加ノードｎが検出された場合、ステップ３２の処理を行い、新規追加ノードｎに対して機密化された暗号コードを用いて正規の送受信ノードであるかどうかの確認を行う。新規追加ノードｎが正規の送受信ノードである場合には、正規である旨の返答があるが、不正な送受信ノードである場合には、なんの返答もない。そこで、ステップ３３で、正規である旨の返答が有ったかどうかの判定を行い、返答有り（ＹＥＳ）の場合は、ステップ３４で新規追加ノードｎは正規の送受信ノードであり、通信ネットワーク２０全体は安全だと判断して各ノード１～ｎ－１に安全である旨の報告を行う。一方、ステップ３３で返答無し（ＮＯ）と判定されたということは、新規追加ノードｎは何らかの不正な送受信ノードだということなので、ステップ３５で各ノード１～ｎ－１に不正送受信ノードの混在を報告する。なお、安全だという報告を受けた各送受信ノード１～ｎ－１は、通常のデータ入出力動作モードとなり、データのやりとりを通信ネットワーク２０上で自由に行う。一方、不正な送受信ノードが混在しているという報告を受けた各送受信ノード１～ｎ－１は、プロテクトデータ入出力動作モードとなり、通信ネットワーク２０を経由してのデータの入出力動作を行わずに、個別の通信回線などを使って正規な送受信ノードとの間でデータのやりとりを行ったり、又は通信ネットワーク２０上に送出するデータ自身にスクランブル処理などの暗号化処理を行って、不正な送受信ノードｎが通信ネットワーク２０上を流れるディジタルデータを読み取ることができないようにする。このような監視ノード１０を正規の送受信ノード１～ｎ－１だけで構成されていた通信ネットワーク２０上に設けることによって、不正な送受信ノードｎが新たに接続された場合に、通信ネートワーク２０上ではディジタルデータの送受信が行われなくなったり、データにスクランブル処理などの暗号化処理が行われるようになるので、ディジタルデータの不正コピーを有効に防止することができる。

【００１６】図１の実施の形態では、監視ノード１０を

通信ネットワーク２０上に設けて、この監視ノード１０によって新規追加ノードの有無を検出したり、正規ノードかどうかの判定を行う場合について説明したが、この監視ノード１０を設けることなく、各送受信ノード１～ｎ－１がそれぞれ図１の監視ノード１０のような動作を行うようにしてもよい。図４はこのように各送受信ノード１～ｎ－１が監視ノード１０と同じ動作を行う場合の一例を示す図であり、図１（Ａ）と異なる点は図４（Ａ）のように通信ネットワーク２０上に監視ノード２０が接続されていない点である。従って、このような場合には、各送受信ノード１～ｎ－１は図４（Ｂ）のような動作を行う。すなわち、各送受信ノード１～ｎ－１は、ステップ４１で通信ネットワーク２０に送受信ノード（新規追加ノード）ｎが新たに接続されたかどうかの判定を行い、検出された（ＹＥＳ）場合は次のステップ４２に進み、そうでない場合はステップ４８に進み、各送受信ノード独自の処理（その他の処理）を行う。ステップ４１で新規追加ノードｎが検出された場合には、ステップ４２で、新規追加ノードｎに対して機密化された暗号コードを用いて正規の送受信ノードであるかどうかの確認を行う。新規追加ノードｎが正規の送受信ノードである場合には、正規である旨の返答があるが、不正な送受信ノードである場合には、なんの返答もない。そこで、ステップ４３で、正規である旨の返答が有ったかどうかの判定を行い、判定結果が返答有り（ＹＥＳ）の場合は、ステップ４４で新規追加ノードｎは正規の送受信ノードであり、通信ネットワーク２０全体は安全だと判断し、ステップ４５で通常のデータ入出力動作モードに設定する。これによって、ステップ４８のその他の処理で通信ネットワーク２０を介してデータの入力動作を行う場合に通常のデータ入出力動作が行われる。一方、ステップ４３で返答無し（ＮＯ）と判定されたということは、新規追加ノードｎは何らかの不正な送受信ノードということなので、ステップ４６で通信ネットワーク２０上に不正な送受信ノードが混在していると判断し、ステップ４７でプロテクトデータ入出力動作モードに設定する。これによって、各送受信ノード１～ｎ－１は、通信ネットワーク２０を経由してデータの入出力動作を行わずに、個別の通信回線などを使って正規な送受信ノードとの間でデータのやりとりを行ったり、又は通信ネットワーク２０上に送出するデータ自身にスクランブル処理などの暗号化処理を行って、不正な送受信ノードが通信ネットワーク２０上を流れるディジタルデータを読み取ることができないようにして、データ伝送を行う。このように各送受信ノードが監視ノードと同様の処理を行うことによって、正規の送受信ノード１～ｎ－１だけで構成されていた通信ネットワーク２０上に不正な送受信ノードｎが接続されると、通信ネートワーク２０上ではディジタルデータの送受信が行われなくなったり、データにスクランブル処理などの暗号化処理が行われるようになるので、ディジタルデータの不正コピーを有効に防止することができる。

【００１７】図１のように通信ネットワーク２０上に監視ノード１０を有する場合は、通信ネットワーク２０上に新たに送受信ノードが追加された場合に、それが正規の機器であるか否かをの判定を行うことができるが、複数の送受信ノードによって予め構成された通信ネットワーク上に監視ノード１０を設けてもその通信ネットワークを構成する各送受信ノードが正規の機器であるか否かの判定を行うことはできない。また、図４のように各送受信ノードが監視ノードと同じ機能を有する場合には、これらの送受信ノードを用いて通信ネットワークを構成することができるが、監視ノードと同じ機能を有しない送受信ノードをこの通信ネットワーク上に接続したとしても、それが有効に動作するという保証がない。すなわち、送受信ノードが正規な機器であり、図１（Ａ）のように正規である旨の返答を返すことはできるが、監視ノードと同じ機能を有していないので、この送受信ノードが通信ネットワーク上に接続された場合には、その通信ネットワークは安全と判断されるが、さらに新規な送受信ノードが追加され、それが不正なものであった場合には、監視ノードと同じ機能を有しない送受信ノードは不正であることを認識できないので、通信ネットワーク全体がプロテクトデータ入出力動作モードに移行したことを認識できずに、データ伝送を有効に行うことができなくなる。そこで、図１の監視ノード１０の機能の一部として、通信ネットワーク上に新規ノードが追加されたかどうかを検出するという機能を各送受信ノードに持たせて、監視ノード１０は各送受信ノードによって検出された新規ノード検出信号に基づいて、新規に接続された送受信ノードに対してはもちろん既存の通信ネットワーク上に接続されている全ての送受信ノードに対して、機密化された暗号コードを用いて正規の機器であるか否かの判定を行うようにした。以下、このような場合の監視ノードと各送受信ノードとの動作の一例を図５及び図６のフローチャートを用いて説明する。

【００１８】ステップ５１では、各送受信ノード１～ｎは、通信ネットワーク２０上に新たに送受信ノード（新規追加ノード）が接続されたかどうか、すなわち新規追加ノードが検出された否かの判定を行い、新規追加ノードが検出された（ＹＥＳ）場合は次のステップ５２に進み、そうでない（ＮＯ）場合はステップ５Ａに進んで各送受信ノード独自の処理（その他の処理）を行う。ここで、送受信ノード１～ｎ－１によって構成される既存の通信ネットワーク２０上に送受信ノードｎが新たに接続された場合は各送受信ノード１～ｎ－１は送受信ノードｎを新規追加ノードとして認識し、逆に送受信ノードｎは送受信ノード１～ｎ－１を新規追加ノードとして認識することになる。従って、このような場合には、送受信ノード１～ｎの全てが新規追加ノードを検出したことに

なるので、各送受信ノード１～ｎはステップ５２の処理を行い、新規追加ノードを検出した旨の確認信号を通信ネットワーク２０上に出力する。各送受信ノードが新規追加ノードを検出した場合に、監視ノード１０は、各送受信ノード１～ｎに対して正規の機器であるかどうかの確認信号を出力したり、通信ネットワーク２０が安全である旨の報告又は通信ネットワーク２０に不正な送受信ノードが混在する旨の報告を行ったりすることになっている。このような監視ノード１０の処理については図６を用いて後述する。そこで、各送受信ノード１～ｎは正規機器の確認信号を受信したかどうかの判定を行い、受信した（ＹＥＳ）場合はステップ５４に進み、そこで正規機器である旨の確認コードを出力する。監視ノード１０から正規機器の確認信号を受信していない（ＮＯ）場合はステップ５５に進む。ステップ５５では、通信ネットワーク全体が安全である旨の報告又は不正な送受信ノードが混在している旨のいずれかの報告が監視ノードから有るかどうかを判定し、報告有り（ＹＥＳ）の場合はステップ５６～ステップ５９でその報告の種類に従って処理を行い、報告無し（ＮＯ）の場合はステップ５３に戻り、監視ノード１０からの報告があるまでステップ５３～ステップ５５の処理を繰り返し実行する。監視ノード１０からの報告が通信ネットワーク２０全体が安全である旨の報告の場合には、ステップ５６でＹＥＳと判定されるので、各送受信ノード１～ｎはステップ５７で通常のデータ入出力動作モードに設定される。これによって、各送受信ノード１～ｎはステップ５Ａのその他の処理で通信ネットワークを介してデータの入力動作を行う場合に通常のデータ入出力動作を行うようになる。一方、監視ノード１０からの報告が通信ネットワーク２０上になんらかの不正な送受信ノードが混在する旨の報告の場合には、各送受信ノード１～ｎの中の正規の機器は、ステップ５９でプロテクトデータ入出力動作モードに設定される。これによって、正規の送受信ノードは、通信ネットワーク２０を経由してのデータの入出力動作を行わずに、個別の通信回線などを使って正規な送受信ノードとの間だけでデータのやりとりを行ったり、又は通信ネットワーク２０上に送出するデータ自身にスクランブル処理などの暗号化処理を行って、不正な送受信ノードが通信ネットワーク２０上を流れるディジタルデータを読み取ることができないようにする。

【００１９】次に、図６のフローチャートを用いて監視ノードの処理動作の一例を説明する。前述のステップ５２のように、新規追加ノードｎが通信ネットワーク２０上に接続されると、それに応じて既存の送受信ノード１～ｎ－１も新規追加ノードｎも新規追加ノードを検出した旨の確認信号を出力するので、監視ノード１０は、ステップ６１で、各送受信ノード１～ｎから出力された確認信号を順次受信し、最初の確認信号を受信してから所定時間内に全ての送受信ノード１～ｎからの確認信号が来たかどうかの判定を行い、ＹＥＳの場合は次のステップ６２に進み、送受信ノード１～ｎの少なくとも１つから確認信号が来なかった（ＮＯ）場合はステップ６５に進む。ステップ６１でＮＯと判定される場合には、新規追加ノードが不正な機器である場合、既存の送受信ノード１～ｎ－１の中に少なくとも１つの不正な機器が含まれていた場合、又は新規追加ノードｎも不正な機器であり、かつ、既存の送受信ノード１～ｎ－１中にも少なくとも１つの不正な機器が含まれていた場合がそれぞれ該当する。従って、これらの場合には、監視ノード１０は、ステップ６５で、通信ネットワーク２０上になんらかの不正な機器が混在していると判断して、不正な送受信ノードが存在する旨の報告を通信ネットワーク２０上に出力する。一方、ステップ６１でＹＥＳと判定されたということは、新規追加ノードｎも含めて全ての送受信ノード１～ｎから確認信号が通信ネットワーク２０上に出力されたということを意味しているので、この段階までででは通信ネットワーク２０上に接続された全ての送受信ノード１～ｎは確認信号を出力することのできる機器であるということができる。そこで、監視ノード１０は、ステップ６２で、機密化された暗号コードを通信ネットワーク２０上に出力して、通信ネットワーク２０上に接続された全ての送受信コード１～ｎが真に正規の機器かどうかの確認を行う。ステップ６３で、通信ネットワーク２０上の全ての送受信ノード１～ｎから正規である旨の返答有りかどうかの判定を行う。すなわち、通信ネットワーク２０上の送受信ノード１～ｎは自分が正規の機器である場合には、正規である旨の返答を通信ネットワーク２０上に出力するので、監視ノード１０は、その正規である旨の返答が全ての送受信ノード１～ｎから来たかどうかを判定し、返答有り（ＹＥＳ）の場合はステップ６４に進み、全ての送受信ノード１～ｎの中の少なくとも１つから正規である旨の返答がない場合には、ステップ６５に進む。ステップ６４では、通信ネットワーク２０上の全ての送受信ノード１～ｎが正規の機器なので、通信ネットワーク２０全体は安全であると判断して、通信ネットワーク２０上に安全である旨の報告をする。ステップ６５は、ステップ６１又はステップ６３でＮＯと判定された場合に行われる処理である。すなわち、ステップ６１でＮＯと判定されたということは、新規追加ノードｎが通信ネットワーク２０上に接続されたにも係わらず送受信ノード１～ｎの中の少なくとも１つから新規追加ノードを検出した旨の確認信号が通信ネットワーク２０上に出力されなかったことを意味する。ステップ６３でＮＯと判定されたということは、ステップ６１ではＹＥＳと判定されたが、機密化された暗号コードを用いた正規機器の判定処理において送受信ノード１～ｎの少なくとも１つから正規である旨の返答が来なかったことを意味する。従って、このような場合には、通信ネットワーク２０上に接続されている送受信ノード１

～ｎの少なくとも１つが何らかの不正な送受信ノードということを意味するので、ステップ６５で通信ネットワーク２０上に不正な送受信ノードが混在していると判断し、不正ノードの混在を示す報告を通信ネットワーク２０上に出力する。この不正ノードの混在を示す報告を受信した各送受信ノード１～ｎの中の正規の送受信ノードは、ステップ５９の処理でプロテクトデータ入出力動作モードに設定する。このように通信ネットワーク上に新規ノードが追加されたかどうかを検出するという機能を各送受信ノードに持たせて、監視ノードは各送受信ノードによって検出された新規ノード検出信号に基づいて、新規に接続された送受信ノードに対してはもちろん既存の通信ネットワーク上に接続されている全ての送受信ノードに対しても、機密化された暗号コードを用いて正規の機器であるか否かの判定を行うようにしたので、複数の送受信ノードによって予め構成された通信ネットワークに監視ノードを接続するだけで、その通信ネットワーク上に不正な送受信ノードが存在することを検出できる。なお、図５の処理では、通信ネットワーク上に送受信ノード１～ｎ－１と監視ノードが予め接続されており、そこに新たな送受信ノードｎが接続された場合に、新規追加ノードの検出を行うように説明したが、通信ネットワークが送受信ノード１～ｎ－１だけで構成されており、そこに監視ノードが新たに接続された場合も同様に送受信ノード１～ｎ－１が図５の処理を行うようにしてもよい。これによって、送受信ノードだけから構成されるネットワーク上に監視ノードを一時的に接続することによって、その通信ネットワークが安全なのか不正な送受信ノードの混在する安全でないのかを判定し、各送受信ノードのデータ入出力モードを通常モード又はプロテクトモードに設定することができる。

【００２０】なお、上述の実施の形態では、ディジタルデータの送信及び受信の可能な複数の送受信ノードによって構成された通信ネットワークについて説明したが、例えば、マイクやキーボードなどのようにディジタルオーディオデータを送信するだけの送信ノードをこのような通信ネットワークに接続する場合には、送信ノードが少なくとも正規の機器であるかどうかの確認信号に対して応答することができるような構成を有していなければならない。しかしながら、送信だけする簡易な送信ノードにこのような構成を付加することは大変なので、監視ノードと送信ノードとの間にルータを設け、送信ノードをこのルータを介して通信ネットワーク２０上に接続するようにした。図７では、マイク７２とキーボード７３が送信ノードである。マイク７２及びキーボード７３は、ディジタルオーディオデータをルータ７１に出力する。ルータ７１は、監視ノード１０を経由して通信ネットワーク２０上にマイク７２及びキーボード７３からのディジタルオーディオデータを出力する。なお、ルータ７１は監視ノード１０を経由して通信ネットワーク２０上のデータを受信し、このデータの中の送受信ノードｎ－１の出力するノーマルサイクルピリオド１２５μｓｅｃの同期信号（ｃｙｃｌｅ　ｓｙｎｃ）だけをマイク７２及びキーボード７３に出力する。マイク７２及びキーボード７３はこの同期信号に応じてディジタルオーディオデータを出力する。図では、ルータ７１からマイク７２及びキーボード７３に出力される同期信号が点線矢印で示されている。また、キーボード７３からのディジタルオーディオデータはスピーカ７４にも出力され、そこでＤ／Ａ変換処理されて発音処理される。また、ルータ７１にも、前述の送受信ノードと同様に、正規の機器であるかどうかの確認信号に対して応答する機能を具備させることによって、ルータ７１を監視ノード１０を経由してでなく、通信ネットワーク２０上に直接接続することが可能となる。

【００２１】なお、上述の実施の形態では、通信ネットワーク２０上に不正な送受信ノードが検出された場合の処理について説明したが、一旦プロテクトデータ入出力動作モードに設定された後に不正な送受信ノードが通信ネットワーク２０上から取り除かれた場合には、それを検出して、通常のデータ入出力動作モードに設定するようにしてもよい。

【００２２】

【発明の効果】この発明によれば、データ自体を暗号化処理などで変更しなくても、不正な機器との間におけるデータのやりとりを行えないようにするができるという優れた効果を奏する。

【図面の簡単な説明】

【図１】　この発明に係る不正コピー防止システムの第１の実施の形態の全体構成と監視ノードが行う処理の一例を示す図である。

【図２】　この発明に係る不正コピー防止システムによって伝送されるデータの構成例を示す図である。

【図３】　この発明に係る不正コピー防止システムを実現するために図１の監視ノードが行う処理の一例を示す図である。

【図４】　この発明に係る不正コピー防止システムの第２の実施の形態の全体構成と各送受信ノードが行う処理の一例を示す図である。

【図５】　この発明に係る不正コピー防止システムの第３の実施の形態において各送受信ノードが行う処理の一例を示す図である。

【図６】　この発明に係る不正コピー防止システムの第３の実施の形態において監視ノードが行う処理の一例を示す図である。

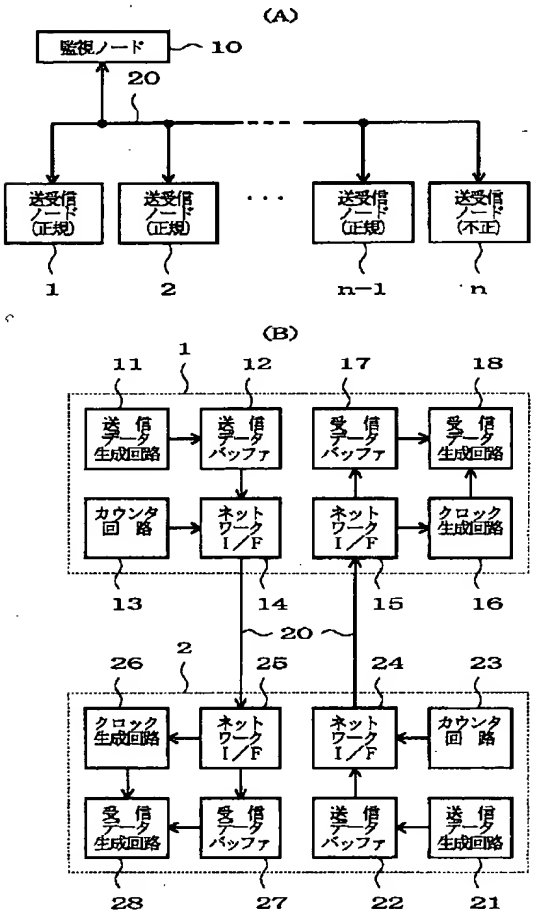
【図７】　この発明に係る不正コピー防止システムの第４の実施の形態の全体構成を示す図である。

【符号の説明】

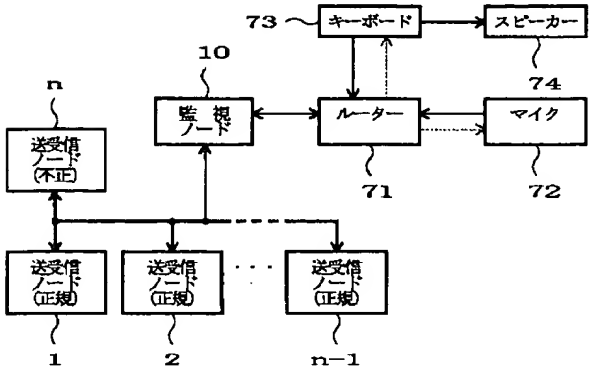
１，２，ｎ－１…送受信ノード（正規）、ｎ…送受信ノード（不正）、１０…監視ノード、２０…通信ネットワ

ーク、１１，２１…送信データ生成回路、１２，２２…送信データバッファ、１３，２３…カウンタ回路、１４，１５，２４，２５…ネットワークインターフェイス、１６，２６…クロック生成回路、１７，２７…受信データバッファ、１８，２８…受信データ生成回路

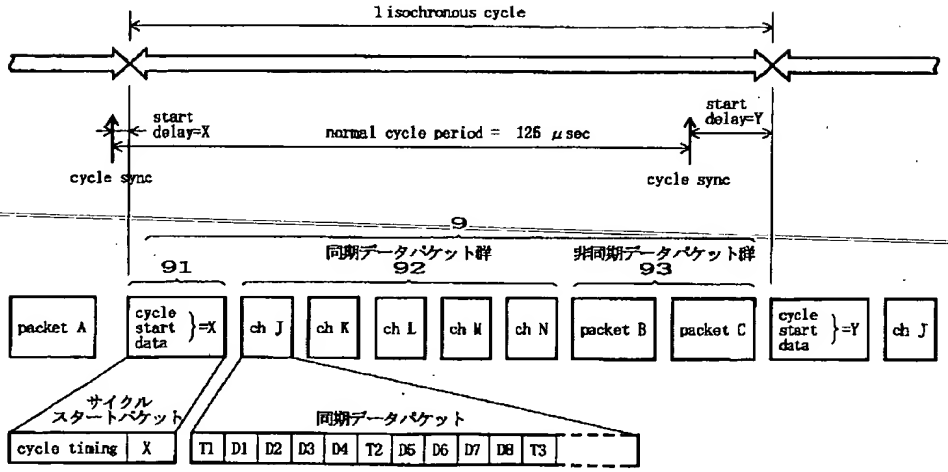
【図１】



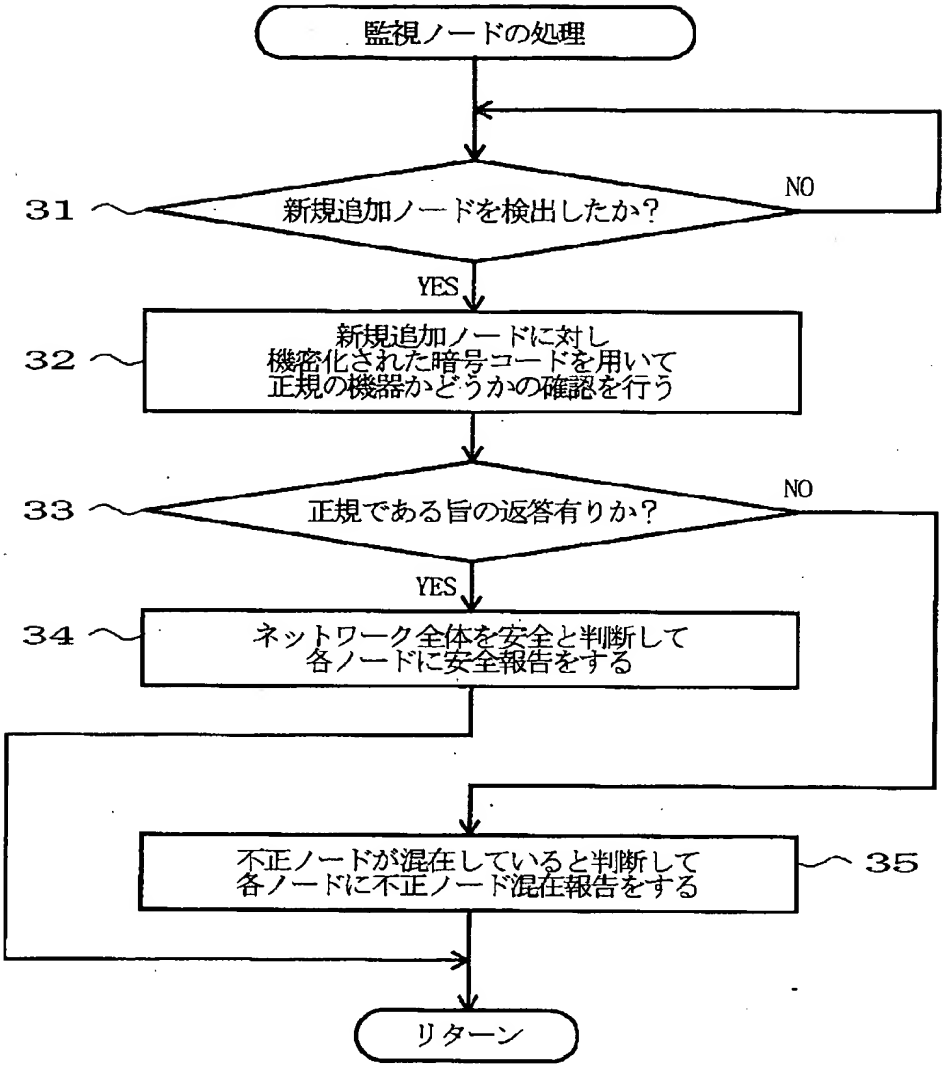
【図７】



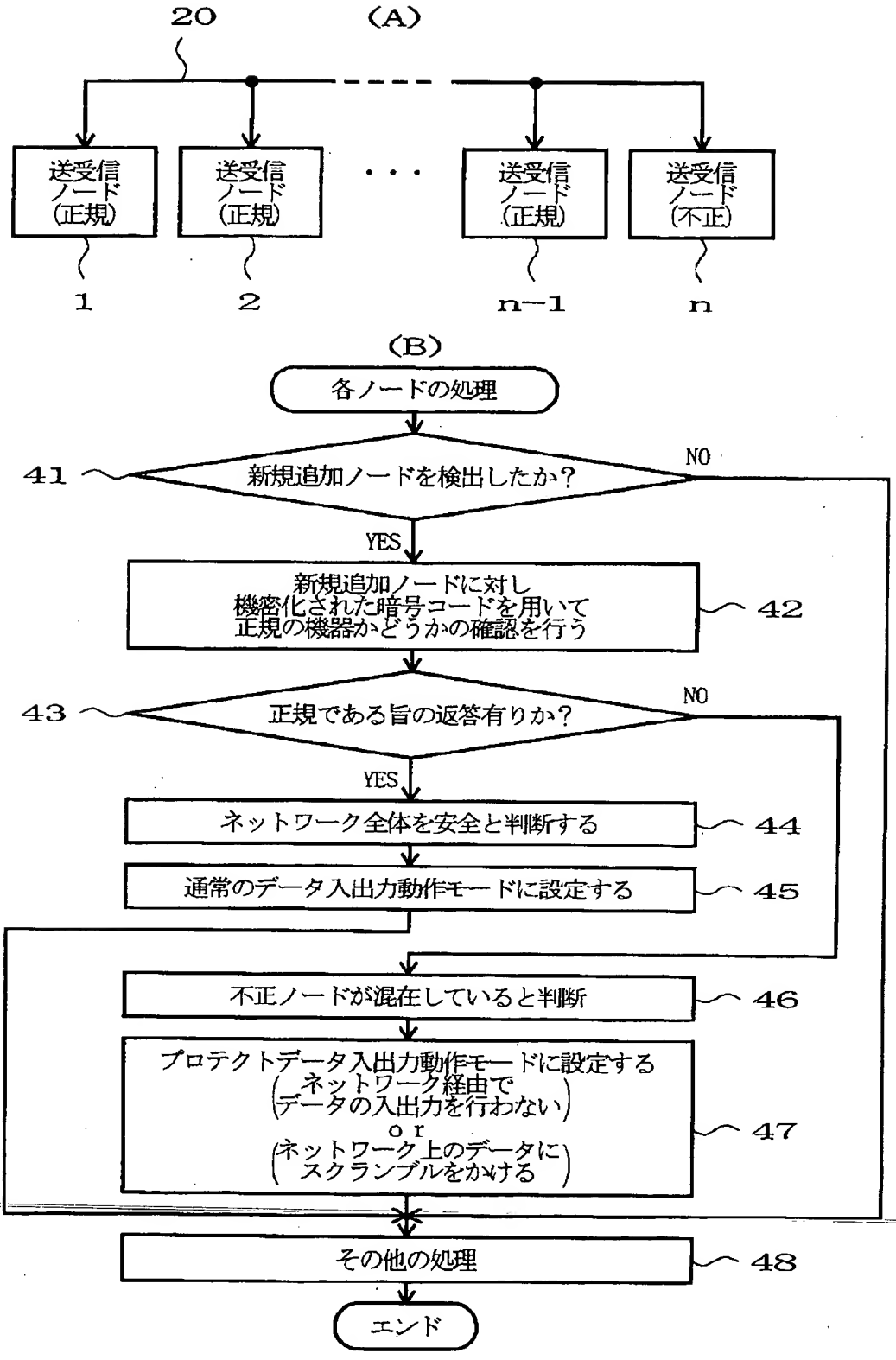
【図２】



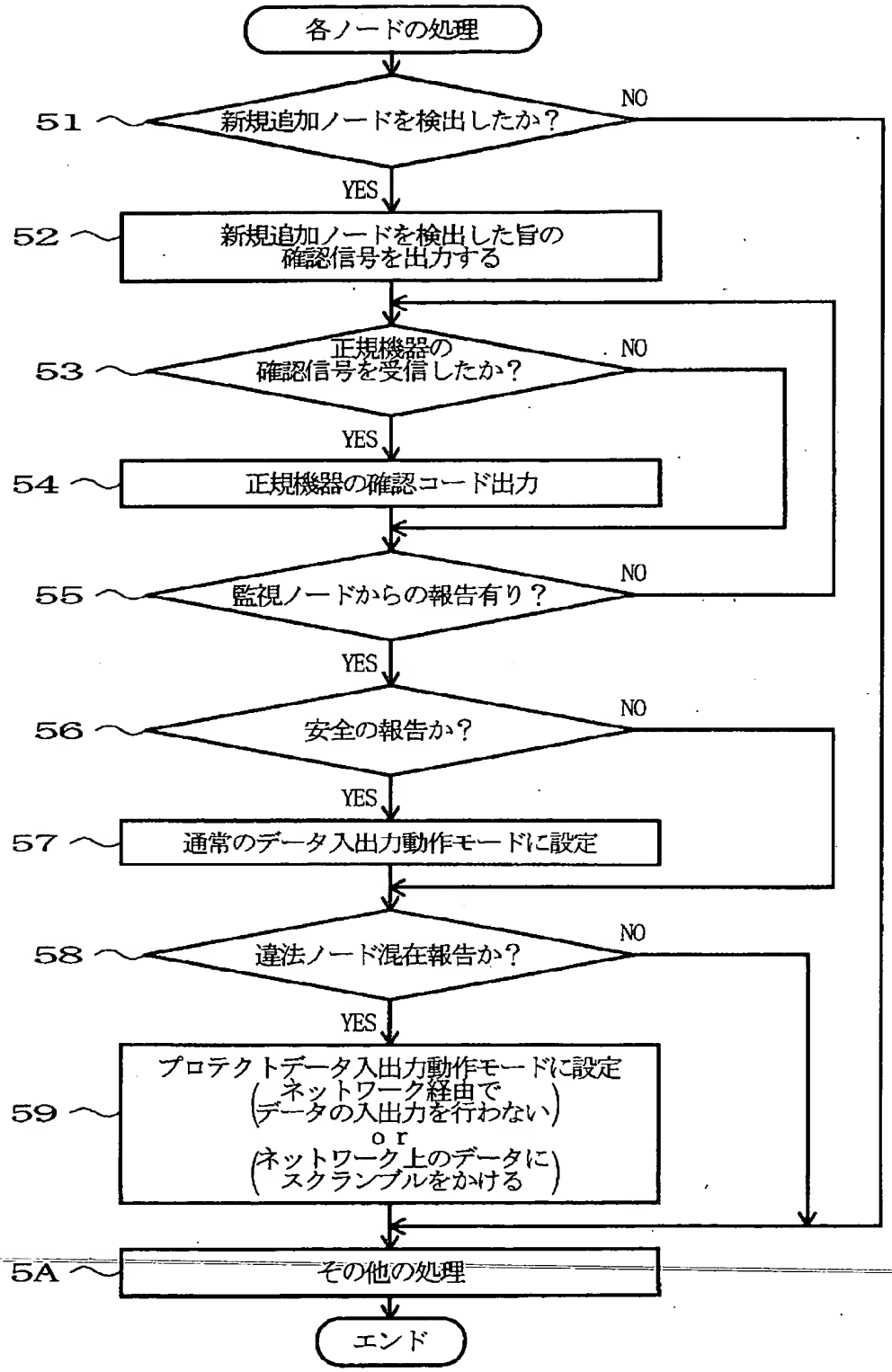
【図3】


監視ノードの処理
31
新規追加ノードを検出したか?
NO
YES
32
新規追加ノードに対し
機密化された暗号コードを用いて
正規の機器かどうかの確認を行う
33
正規である旨の返答有りか?
NO
YES
34
ネットワーク全体を安全と判断して
各ノードに安全報告をする
不正ノードが混在していると判断して
各ノードに不正ノード混在報告をする
35
リターン

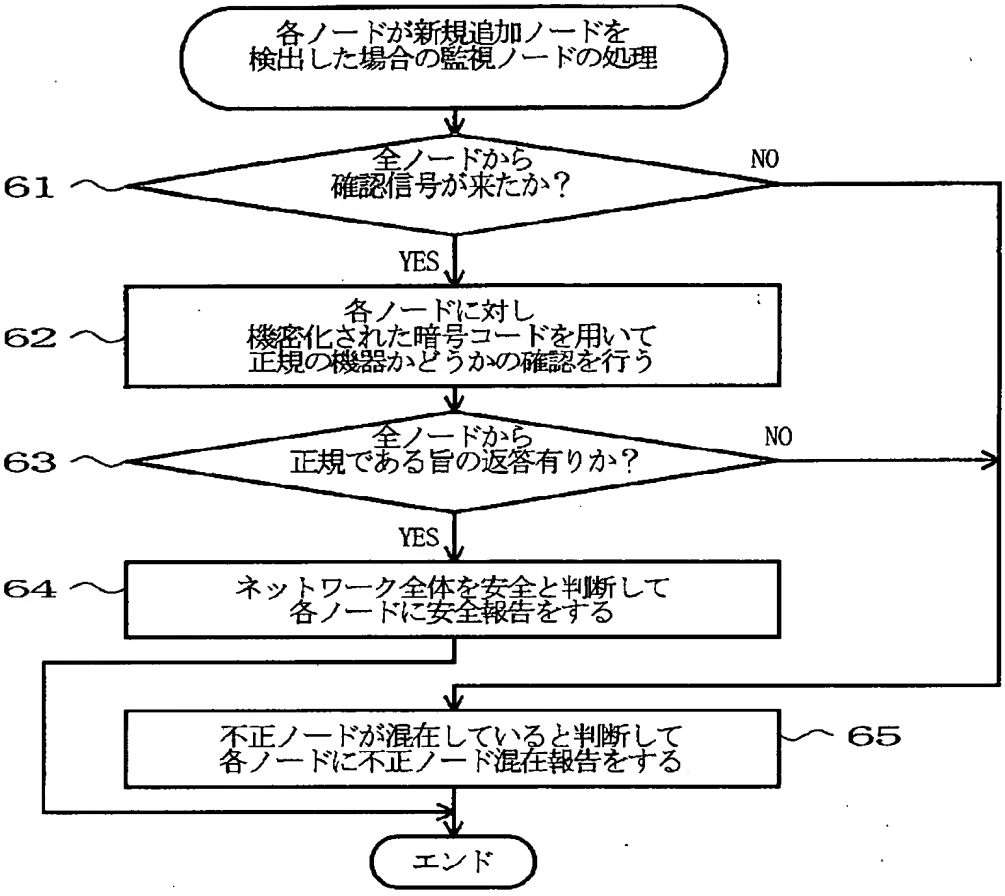
【図4】


20
(A)
送受信ノード(正規)
送受信ノード(正規)
送受信ノード(正規)
送受信ノード(不正)
1
2
n-1
n
(B)
各ノードの処理
41
新規追加ノードを検出したか?
NO
YES
新規追加ノードに対し機密化された暗号コードを用いて正規の機器かどうかの確認を行う
42
43
正規である旨の返答有りか?
NO
YES
ネットワーク全体を安全と判断する
44
通常のデータ入出力動作モードに設定する
45
不正ノードが混在していると判断
46
プロテクトデータ入出力動作モードに設定する
(ネットワーク経由でデータの入出力を行わない)
or
(ネットワーク上のデータにスクランブルをかける)
47
その他の処理
48
エンド

【図5】


各ノードの処理
51
新規追加ノードを検出したか？
NO
YES
52
新規追加ノードを検出した旨の
確認信号を出力する
53
正規機器の
確認信号を受信したか？
NO
YES
54
正規機器の確認コード出力
55
監視ノードからの報告有り？
NO
YES
56
安全の報告か？
NO
YES
57
通常のデータ入出力動作モードに設定
58
違法ノード混在報告か？
NO
YES
59
プロテクトデータ入出力動作モードに設定
(ネットワーク経由で
データの入出力を行わない)
or
(ネットワーク上のデータに
スクランブルをかける)
5A
その他の処理
エンド

【図6】


各ノードが新規追加ノードを
検出した場合の監視ノードの処理
61
全ノードから
確認信号が来たか？
NO
YES
62
各ノードに対し
機密化された暗号コードを用いて
正規の機器かどうかの確認を行う
63
全ノードから
正規である旨の返答有りか？
NO
YES
64
ネットワーク全体を安全と判断して
各ノードに安全報告をする
不正ノードが混在していると判断して
各ノードに不正ノード混在報告をする
65
エンド